Leçon 12 : Nombres premiers ; Existence et unicité de la décomposition d'un nombre en facteurs premiers. Infinitude de l'ensemble des nombres premiers. Exemple(s) d'algorithme(s) de recherche de nombres premiers. Calculatrice

---

Niveau : Terminale S spécialité

Prérequis : - division euclidienne
- pgcd / ppcm
- nb premiers entre eux (thm de Gauss)
- (raisonnement par récurrence)
- congruence

I. Nombres premiers

1. Définition

Définition : un entier naturel n supérieur ou égal à 2 est dit premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui-même, sinon on dit qu'il est composé.

Ex. Mq les nbs premiers s'écrivent de la forme $6k-1$, $6k+5$.

oral : on peut étendre la définition aux entiers relatifs en disant qu'un entier négatif ≤ -2 est premier si $-n$ est premier.

oral : La déf. donne immédiatement que 2 nb premiers $\neq$ sont premiers entre eux.

Exemples : 2 est le seul nombre premier pair.
3, 5, 7, 11 sont des nombres premiers.
8, 15 ne sont pas des nombres premiers.

2. Propriétés

Proposition
(*) ~~Théorème~~ : Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier.

Proposition
(1) ~~Théorème~~ : Un entier naturel supérieur ou égal à 2 est premier si et seulement si il est premier avec tout nombre qu'il ne divise pas.

oral
Conséquence : Tout nombre premier p est premier avec tous les entiers naturels compris entre 1 et $(p-1)$.

(2) Lemme d'Euclide
~~Théorème~~ : si un nombre premier divise un produit de 2 facteurs, alors il divise l'un des facteurs.

oral : * la réciproque est également vraie c.à.d que si pour tout couple (b,c) d'entiers naturels non nuls $p \mid bc \Rightarrow (p \mid b$ ou $p \mid c)$ alors p est premier.
* Par récurrence sur le nb de facteurs du produit, on a :

(3) Corollaire : Si un nombre premier divise un produit de facteurs, alors il divise l'un des facteurs.

Si p est premier, $\forall k \in [\![1, p-1]\!]$ $p \mid \binom{p}{k}$ b).

II - Décomposition en facteurs premiers

1. Théorème

Théorème fondamental (4) : Tout entier naturel supérieur ou égal à 2 admet une décomposition en facteurs premiers et celle-ci est unique à l'ordre près. Autrement dit, pour $n \in \mathbb{N} \setminus \{0,1\}$, il existe, uniques : $N \in \mathbb{N}^*$, $p_1, \dots, p_N$ entiers premiers distincts 2 à 2 et $r_1, \dots r_N$ dans $\mathbb{N}^*$ tels que $n = \prod_{i=1}^{N} p_i^{r_i}$.

Preuve (juste existence car unicité pas au programme de TS)
Par récurrence.
HR(n) : tout nombre $k \leq n$ vérifie " k admet une décomposition en facteurs premiers ".

* $n = 2$ la récurrence est fondée.
* supposons la propriété vraie jusqu'au rang n. Montrons-la au rang $n+1$.
  → soit $n+1$ est premier alors HR(n+1) est vérifiée.
  → soit $n+1$ est composé.
  Par le théorème (*), il existe p premier tq $(n+1) = p \cdot a$ avec $p > 1$.
  Donc $a \leq n$.
  Par hypothèse de récurrence, a admet une décomposition en facteurs premiers. Donc $(n+1)$ aussi.
  La propriété est vérifiée au rang $(n+1)$. Elle est héréditaire donc démontrée. □

Exemples : $18 = 2 \times 3^2$
$40 = 2^3 \times 5$
$105 = 3 \times 5 \times 7$

2. Application aux pgcd et ppcm.

1) Proposition ⑤ : soient a et b 2 entiers naturels supérieurs ou égals à 2 tels que $a = \prod_{i=1}^{N} p_i^{m_i}$ $b = \prod_{i=1}^{N} p_i^{n_i}$ où $N \in \mathbb{N}^*$

$p_1, \dots, p_N$ nombres premiers distincts 2 à 2
$m_1, \dots, m_N, n_1, \dots, n_N$ dans $\mathbb{N}$ pas forcément les m facteurs premiers de il peut $\exists\ m_i = 0$ ou $n_i = 0$.

Alors $pgcd(a,b) = \prod_{i=1}^{N} p_i^{\min(m_i, n_i)}$

$ppcm(a,b) = \prod_{i=1}^{N} p_i^{\max(m_i, n_i)}$

Exemples : $1998 = 2 \cdot 3^3 \cdot 37$
$1968 = 2^4 \cdot 3 \cdot 41$
donc $pgcd(1968, 1998) = 2 \cdot 3$
$ppcm(1968, 1998) = 2^4 \cdot 3^3 \cdot 37 \cdot 41$

2) Nbre de diviseurs $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ $d(n) = \prod_{i=1}^{N} (1+\alpha_i)$

III. Infinitude de l'ensemble des nombres premiers

Théorème : L'ensemble des nombres premiers est infini.

Preuve
Par l'absurde, on suppose que l'ensemble P des nombres premiers est fini.
Il existe $n \in \mathbb{N}^*$ tel que $P = \{p_1, \dots, p_n\}$.
on pose $N = p_1 \times p_2 \times \dots \times p_n + 1$, on a $N \geq 2$.
Par le théorème (*), il existe p premier qui divise N.
or $p \in \{p_1, \dots, p_n\}$
donc p divise $p_1 \times \dots \times p_n$
$1 = N - p_1 \times \dots \times p_n$ donc $p \mid 1$ impossible car p premier ≥ 2.
Ex. Il existe une infinité de nombre premier de la forme $(4k+3)$. □

IV. Exemples d'algorithmes de recherche de nombres premiers.

1. Premier algorithme

Proposition ⑥ : tout entier naturel n composé supérieur ou égal à 2 admet au moins un diviseur premier q tel que $q^2 \leq n$.
oral : c.à.d $q \leq \sqrt{n}$.

Algorithme : calculatrice :

```
premier()
Prgm
Prompt n
2 → q
While q² ≤ n
If mod(n, q) = 0 Then
Disp " n n'est pas premier "
Exit
Else
q+1 → q
EndIf
End While
If q² > n
Disp " n est premier "
EndPrgm
```

commentaires

lire n
on fixe q à 2
tant que $q^2 \leq n$ faire
si q | n (ie reste de la div° de n par q = 0)
écrire " n n'est pas premier "
sortir de la boucle tant que
sinon
faire q = q+1

fin boucle tant que
si $q^2 > n$
écrire " n est premier ".

oral: on peut améliorer l'algorithme en testant seulement les diviseurs impairs et 2.

Exemples : 2549 est premier
1457 n'est pas premier.

2. Deuxième algorithme : crible d'Eratosthène

Il permet d'obtenir la liste des nombres premiers entre 2 et n ($n \geq 2$).
oral: on part du fait qu'un diviseur propre d'un nombre n (c'est à dire distinct de ce nombre) est inférieur à n.

- On écrit la liste de tous les entiers de 2 à n
- commençant par 2, on barre tous les multiples de 2
- L'entier 3 n'a pas été barré (il ne peut être multiple des entiers qui le précède, sinon on l'aurait supprimé), il est donc premier, on barre alors tous les multiples de 3

⋮

- on barre tous les multiples de p avec p le plus petit entier non encore barré.

Exemple :

②	③	~~4~~	⑤	~~6~~	⑦	~~8~~	~~9~~	~~10~~
⑪	~~12~~	⑬	~~14~~	~~15~~	~~16~~	⑰	~~18~~	⑲	~~20~~
~~21~~	~~22~~	㉓	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	㉙	~~30~~

oral: on peut s'arrêter à 7 car $7^2 > 30$ avec la proposition de l'algo précédent.

→ si encore du temps sinon c'est pas grave.

V. Théorème de Fermat

Théorème : soit p un nombre premier. Quel que soit l'entier a premier avec p on a : $a^{p-1} \equiv 1 \mod p$.

Corollaire : soit p un nombre premier, quel que soit $a \in \mathbb{N}$, on a : $a^p \equiv a \mod p$.

oral: ce qui nous donne un critère pour dire qu'un nombre n'est pas premier. si on trouve a tq $a^p \not\equiv a \mod p$ alors p n'est pas premier.

Exemple : 147 n'est pas premier car $2^{147} \not\equiv 2 \mod 147$.
($\equiv 50 \mod 147$)

Ccl: La recherche de gd nbre premier a un interet
de la cryptographie en particulier pr le système
RSA. On a pensé que cela se pourrait à l'aide des nbres de
fermat qui sécrit $2^{2^n}+1$ mais qui s'avère ne pas être premier pr

Leçon 12 : Preuves + compléments

Théorème (*)

soit $n \geq 2$
L'ensemble des diviseurs naturels de n distincts de 1 contient n et n'est donc pas vide ; il admet un plus petit élément que l'on nomme p.
soit d un diviseur naturel de p distinct de 1 (il en existe au moins un qui est p lui-même).
On a $d \leq p$; de plus, $d \mid p$ et $p \mid n$ donc $d \mid n$
d est donc un diviseur naturel de n distinct de 1, d'où $d \geq p$, par définition de p.
On conclut donc à l'égalité $d = p$.
p admet donc un unique diviseur naturel distinct de 1 : p.
p est donc un nombre premier qui divise n.

(1) Théorème

$\Rightarrow$) on suppose p nombre premier.
soit n un entier tq $p \nmid n$.
Alors $\text{pgcd}(p, n) \in \{1, p\}$
or $p \nmid n$ donc $\text{pgcd}(p, n) = 1$. Ainsi p et n sont premiers entre eux.

$\Leftarrow$) on suppose que p est premier avec tout nb qu'il ne divise pas
supposons $p = p_1 p_2$ $\quad p_1, p_2 < p$
$p \nmid p_1$ donc $p_1 \wedge p = 1$
Gauss : $p \mid p_1 p_2$ et $p \wedge p_1 = 1$
donc $p \mid p_2$ or $p_2 < p$ $\longrightarrow\!\!\leftarrow$ donc p premier.

(2) Théorème

soit p premier
on suppose $p \mid ab$.
. si $p \mid a$ ok
. sinon $p \nmid a$ alors $\text{pgcd}(a, p) = 1$
donc $p \mid b$ (par Gauss)

Corollaire (3)

par récurrence sur le nb de facteurs du produit.
. si $n = 2$, thm précédent ok
. supposons la propriété vraie jusqu'au rang $n-1$
On suppose p divise $a_1 a_2 \dots a_n$
. si $p \mid a_n$ ok la récurrence est bouclée
. sinon $\begin{cases} p \nmid a_n \\ p \mid a_1 a_2 \dots a_n \end{cases}$ donc $p \mid a_1 a_2 \dots a_{n-1}$ (Gauss)
on peut appliquer l'hypothèse de récurrence, donc p divise l'un des a_i, $i \in \{1, \dots, n-1\}$.
La propriété est vraie au rang n.
Elle est héréditaire donc démontrée par récurrence.

Théorème fondamental (4)

Unicité : par récurrence sur n.
* $n = 2$, si $2 = q_1^{\beta_1} \dots q_m^{\beta_m}$ montre que q_i divise 2 pour tout i.
autrement dit $m = 1$, $q_1 = 2$ et $\beta_1 = 1$.
* Supposons que l'unicité soit démontrée jusqu'au rang n.
et considérons les écritures $n+1 = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_m^{\beta_m}$ avec $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_m \in \mathbb{N}^*$ et où les $p_1, \dots, p_k, q_1, \dots, q_m \in \mathbb{N}$ sont premiers.
donc p_k divise $q_1^{\beta_1} \dots q_m^{\beta_m}$ donc divise l'un des q_i, par exemple $p_k \mid q_m$.

comme p_k premier, cela entraîne $p_k = q_m$

et $\frac{n+1}{p_k} = p_1^{\alpha_1} \dots p_k^{\alpha_k - 1} = q_1^{\beta_1} \dots q_m^{\beta_m - 1}$

on applique l'hypothèse récurrente à cette décomposition en distinguant deux cas pour que les exposants soient tous strictement positifs :

si $\alpha_k = 1$ alors $\beta_m = 1$ autrement q_m diviserait l'un des p_i avec $i \neq k$, absurde

si $\alpha_k > 1$ alors $\beta_m > 1$ autrement p_k diviserait l'un des q_i avec $i \neq m$, absurde.

Proposition: ⑤

Il est évident que le nombre $d = \prod_{i=1}^{N} p_i^{\min(m_i, n_i)}$ divise a et b.

Par ailleurs, tout nombre divisant a et b a pour décomposition en produit de facteurs premiers $\prod_{i=1}^{N} p_i^{\delta_i}$ où $\delta_i \leq m_i$ et $\delta_i \leq n_i$

on a donc $\delta_i \leq \min(m_i, n_i)$ et par suite, ce nombre divise d

donc d est le pgcd de a et b.

Même raisonnement avec le ppcm : $m = \prod_{i=1}^{N} p_i^{\max(m_i, n_i)}$

→ a et b divise m, donc m est multiple de a et b.

→ si a et b divise un entier N, alors N est multiple de m.

Proposition ⑥

l'ensemble des diviseurs d de n tels que $2 \leq d < n$ n'est pas vide.

et on sait qu'il existe un nombre premier p qui est le plus petit élément des diviseurs de n tq $n = p \times q$ avec $2 \leq p \leq q$ par déf de p.

donc $p^2 \leq pq = n$.

Théorème de Fermat :

voir leçon 10 : congruences dans $\mathbb{Z}$ - Anneaux $\mathbb{Z}/n\mathbb{Z}$.

il existe c tel que $b = ac$. Si l'on note $c = wp_1^{\gamma_1}...p_n^{\gamma_n}$ la décomposition en produit de facteurs premiers de c, et si l'on utilise l'unicité de la décomposition de b, cela équivaut à l'existence d'entiers naturels γ_i tels que $\beta_i = \alpha_i + \gamma_i$ pour tout i.
Par conséquent, l'entier $d = wp_1^{\gamma_1}...p_n^{\gamma_n}$ divise a et b si, et seulement si, d divise $\delta = p_1^{\text{Inf}(\alpha_1,\beta_1)}...p_n^{\text{Inf}(\alpha_n,\beta_n)}$, et δ sera un pgcd de a, b. En recommençant avec le ppcm, on obtient les formules :

$$\begin{cases} \text{pgcd}\,(a,b) = p_1^{\text{Inf}(\alpha_1,\beta_1)}...p_n^{\text{Inf}(\alpha_n,\beta_n)}, \\ \text{ppcm}\,(a,b) = p_1^{\text{Sup}(\alpha_1,\beta_1)}...p_n^{\text{Sup}(\alpha_n,\beta_n)}. \end{cases}$$

6 Remarques et compléments

6.1 Table de Sundaram

La table de Sundaram est un tableau carré infini construit de la façon suivante. La 0-ième ligne et la 0-ième colonne du tableau contiennent les termes de la progression arithmétique de premier terme 4 et de raison 3. La première ligne contient, de gauche à droite, les termes de la progression arithmétique de premier terme 7 et de raison 5. Et ainsi de suite... La i-ème ligne contient, de gauche à droite, les termes de la progression arithmétique de raison $3 + 2i$.

	colonne 0	colonne 1	colonne 2	colonne 3	$\cdots$	
ligne 0	4	7	10	13	$\cdots$	$\longleftarrow$ raison 3
ligne 1	7	12	17	22	$\cdots$	$\longleftarrow$ raison 5
ligne 2	10	17	24	31	$\cdots$	$\longleftarrow$ raison 7
$\vdots$						$\vdots$
ligne i	$4+3i$	$\cdots$			$\cdots$	$\longleftarrow$ raison $3+2i$
$\vdots$						

Le nombre inscrit dans la i-ème ligne et la j-ème colonne sera

$$N_{ij} = 4 + 3i + (3 + 2i)\, j,$$

de sorte que $N_{ij} = N_{ji}$ et que le tableau soit symétrique par rapport à sa diagonale principale.

On peut alors déterminer si un nombre M donné est premier. Pour cela ont regarde d'abord si $M = 2$. Dans le cas où $M \neq 2$, on détermine N tel que $M = 2N + 1$ et l'on utilise le Théorème :

Théorème 3 *Soit $N \in \mathbb{N}^*$. Alors $2N+1$ n'est pas premier si et seulement si N est inscrit dans le tableau ci-dessus.*

Preuve : On a

$$2N_{ij} + 1 = 8 + 6i + 6j + 4ij = (3 + 2i)\,(3 + 2j)$$

donc $2N_{ij} + 1$ n'est pas premier. Réciproquement, tout nombre $2N + 1$ qui n'est pas premier s'écrit $2N + 1 = ab$ avec a et b impairs et ≥ 3, donc s'écrit aussi sous la forme $2N + 1 = (3 + 2i)\,(3 + 2j)$ avec $i \geq 0$ et $j \geq 0$. Le calcul ci-dessus montre alors que $N = N_{ij}$. ■